CLAIMS

1. A component for a computer, the component comprising a firmware element operable to perform a security check to verify the computer is connected to an authorised network, the security check comprising the steps of:

generating a random number,

encrypting the random number with a public key of a public/private key pair associated with the network,

transmitting the encrypted random number to a network device via the network,

receiving a response comprising a number from the network device, and

permitting operation of at least a subsystem of the computer if the response is in accordance with the random number,

the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device.

2. A component according to claim 1 wherein the firmware element comprises a BIOS.

3. A component according to claim 2 wherein the firmware element is operable to perform a security check as part of a boot process.

4. A component according to claim 2 wherein the firmware element is operable to prevent operation of the computer if a valid response is not received.

5. A component according to claim 2 wherein the BIOS comprises a boot block and wherein the firmware element is stored in the boot block.

6 A component according to claim 1 wherein the firmware element comprises a controller for a peripheral.

7. A component according to claim 6 wherein the firmware element is operable to perform a security check in response to a transition to an operating state.

8. A component according to claim 6 wherein the firmware element is operable to prevent operation of the peripheral if a valid response is not received.

9. A component according to claim 6 wherein the network enquiry is transmitted to a BIOS of the computer for transmission to the network device.

10. A component for a computer, the component comprising a firmware element operable to

generate a random number,

encrypt the random number with a public key of a public/private key pair associated with an authorised network,

transmit the encrypted random number to a network device via the network,

receive a response comprising a number from the network device,

compare the random number transmitted to the network device with the number in the response; and

permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device.

11. A BIOS for a computer, the BIOS being operable to perform a security check to verify the computer is connected to an authorised network as part of a boot process, the security check comprising the steps of;

generating a random number,

encrypting the random number with a public key of a public/private key pair associated with the network,

transmitting the encrypted random number to a network device via the network,

receiving a response comprising a number from the network device, and

comparing the random number transmitted to the network device with the number in the response; and

preventing continuation of the boot process if the number in the response does not match the random number transmitted to the network device.

12. A computer comprising a firmware element operable to perform a security check to verify the computer is connected to an authorised network, the security check comprising the steps of:

generating a random number,

encrypting the random number with a public key of a public/private key pair associated with the network,

transmitting the encrypted random number to a network device via the network,

receiving a response comprising a number from the network device, and

permitting operation of at least a subsystem of the computer if the response is in accordance with the random number,

the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device.

13. A computer according to claim 12 wherein the firmware comprises a BIOS.

14. A computer according to claim 13 wherein the firmware element is operable to perform a security check as part of a boot process.

15. A computer according to claim 13 wherein the firmware element is operable to prevent operation of the computer if a valid response is not received.

16. A computer according to claim 13 wherein the BIOS comprises a boot block and wherein the firmware element is stored in the boot block.

17. In combination, a computer comprising an element operable to perform a security check to verify the computer is connected to an authorised network and a network device operable to receive a network enquiry from the computer over a network, the element being operable to;

generate a random number,

encrypt the random number with a public key of a public/private key pair associated with the network, and

transmit the encrypted random number to the network device via the network,

the network device being operable to;

receive the encrypted random number from the computer,

decrypt the encrypted random number using the private key of the public-private key pair,

generate a response comprising the random number and transmit the response to the computer;

the element being operable to;

receive the response comprising from the network device,

compare the random number transmitted to the network device with the number in the response; and

permit operation of at least a subsystem of the computer if the number in the response matches the random number transmitted to the network device.